WE CLAIM:

1. A computer program product comprising a computer program operable to control a computer to generate banned program identifying data indicative of one or more computer programs to be banned from use, said computer program comprising:

(i) user controlled program specifying logic operable to specify one or more computer programs to be banned from use; and

(ii) banned program identifying data generating logic responsive to said user controlled program specifying logic to generate banned program identifying data for said one or more computer programs to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use.

2. A computer program product as claimed in claim 1, wherein said banned program identifying data is encrypted with a private key.

3. A computer program product as claimed in claim 2, wherein said private key is a PGP private key.

4. A computer program product as claimed in claim 1, wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were a computer virus.

5. A computer program product as claimed in claim 4, wherein said banned program identifying data includes heuristic data identifying one or more behavioural characteristics of one or more computer programs banned from use such that variants of said one or more computer programs banned from use that share said behavioural characteristics may also be identified.

6. A computer program product as claimed in claim 1, wherein said banned program identifying data comprises data identifying permitted computer programs

with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

7. A computer program product comprising a computer program operable to control a computer to ban from use one or more computer programs, said computer program comprising:

(i) anti computer virus logic responsive to user generated banned program identifying data for said one or more computer programs to be banned from use to identify computer programs banned from use.

8. A computer program product as claimed in claim 7, wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use.

9. A computer program product as claimed in claim 8, wherein said private key is a PGP private key and said public key is a corresponding PGP public key.

10. A computer program product as claimed in claim 8, wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

11. A computer program product as claimed in claim 7, wherein when a banned computer program is identified, one or more banned program actions are triggered, said banned program actions comprising at least one of:

(i) issuing an alert message indicating identification of a banned computer program;

(ii) denying access to said banned computer program;

(iii) encrypting said banned computer program; and

(iv) deleting said banned computer program.

12. A computer program product as claimed in claim 7, wherein said anti computer virus logic responses to an absence of said user generated banned program identifying data by performing at least one of:

(i) issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii) restoring said user generated banned program identifying data from a remote source;

(iii) disabling a computer upon which said anti computer virus logic is executing.

13. A computer program product as claimed in claim 7, wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use.

14. A computer program product as claimed in claim 7, wherein said user generated banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

15. A method of generating banned program identifying data indicative of one or more computer programs to be banned from use, said method comprising the steps of:

(i) user specifying one or more computer programs to be banned from use; and

(ii) generating banned program identifying data for said one or more computer programs to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use.

16. A method as claimed in claim 15, wherein said banned program identifying data is encrypted with a private key.

17. A method as claimed in claim 16, wherein said private key is a PGP private key.

18. A method as claimed in claim 15, wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were a computer virus.

19. A method as claimed in claim 18, wherein said banned program identifying data includes heuristic data identifying one or more behavioural characteristics of one or more computer programs banned from use such that variants of said one or more computer programs banned from use that share said behavioural characteristics may also be identified.

20. A method as claimed in claim 15, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

21. A method for banning from use one or more computer programs, said method comprising the step of:

(i) in response to user generated banned program identifying data for said one or more computer programs to be banned from use, operating anti computer virus logic to identify computer programs banned from use.

22. A method as claimed in claim 21, wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use.

23. A method as claimed in claim 22, wherein said private key is a PGP private key and said public key is a corresponding PGP public key.

24. A method as claimed in claim 22, wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

25. A method as claimed in claim 21, wherein when a banned computer program is identified, one or more banned program actions are triggered, said banned program actions comprising at least one of:

(i) issuing an alert message indicating identification of a banned computer program;

(ii) denying access to said banned computer program;

(iii) encrypting said banned computer program; and

(iv) deleting said banned computer program.

26. A method as claimed in claim 21, wherein said anti computer virus logic responses to an absence of said user generated banned program identifying data by performing at least one of:

(i) issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii) restoring said user generated banned program identifying data from a remote source;

(iii) disabling a computer upon which said anti computer virus logic is executing.

27. A method as claimed in claim 21, wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use.

28. A method as claimed in claim 21, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

29. Apparatus for generating banned program identifying data indicative of one or more computer programs to be banned from use, said apparatus comprising:

(i) a user controlled program specifier operable to specify one or more computer programs to be banned from use; and

(ii) banned program identifying data generator responsive to said user controlled program specifier to generate banned program identifying data for said one or more computer programs to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use.

30. Apparatus as claimed in claim 29, wherein said banned program identifying data is encrypted with a private key.

31. Apparatus as claimed in claim 30, wherein said private key is a PGP private key.

32. Apparatus as claimed in claim 29, wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were a computer virus.

33. Apparatus as claimed in claim 32, wherein said banned program identifying data includes heuristic data identifying one or more behavioural characteristics of one or more computer programs banned from use such that variants of said one or more computer programs banned from use that share said behavioural characteristics may also be identified.

34. Apparatus as claimed in claim 29, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

35. Apparatus for banning from use one or more computer programs, said apparatus comprising:

(i) an anti computer virus system responsive to user generated banned program identifying data for said one or more computer programs to be banned from use to identify computer programs banned from use.

36. Apparatus as claimed in claim 35, wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use.

37. Apparatus as claimed in claim 36, wherein said private key is a PGP private key and said public key is a corresponding PGP public key.

38. Apparatus as claimed in claim 36, wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

39. Apparatus as claimed in claim 35, wherein when a banned computer program is identified, one or more banned program actions are triggered, said banned program actions comprising at least one of:

(i) issuing an alert message indicating identification of a banned computer program;

(ii) denying access to said banned computer program;

(iii) encrypting said banned computer program; and

(iv) deleting said banned computer program.

40. Apparatus as claimed in claim 35, wherein said anti computer virus system responses to an absence of said user generated banned program identifying data by performing at least one of:

(i) issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii) restoring said user generated banned program identifying data from a remote source;

(iii) disabling a computer upon which said anti computer virus logic is executing.

41. Apparatus as claimed in claim 35, wherein said anti computer virus system is executable as a separate instance solely to identify computer programs banned from use.

42. Apparatus as claimed in claim 35, wherein said user generated banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.